CLAIMS:

1. A method for a party participating in a secure multiparty multiplication protocol between participants, the protocol being arranged to compute the product of private first data and encrypted second data, wherein the protocol comprises a subprotocol comprising the steps of

- the party (100) obtaining first data (101), which is either
  - private first data or
  - first data from a two-valued domain,
- the party obtaining encrypted second data (102),
- the party computing encrypted output data (103) which comprises a randomized encryption of the product of the first data and the second data, using a discrete log based cryptosystem, and
- the party generating a proof (104) being arranged to show that the encrypted output data is correct.

2. Method according to claim 1, wherein the first data is random data from a two-valued domain.

3. Method according to claim 1, wherein the discrete log based cryptosystem is the ElGamal cryptosystem.

4. The method according to claim 1, wherein the encrypted data are Pederson commitments.

5 The method according to claim 1, wherein the protocol further comprises the further step of the party transmitting the proof to at least one of the other participants.

6. The method according to claim 1, wherein the protocol comprises the further step of the party transmitting the encrypted output data to at least one of the other participants.

7. The method according to claim 1, wherein the protocol is executed between two parties.

8. A device (200) being arranged for implementing the method according to claim 1.

9. A computer program product (210), for enabling multiparty computations, having computer executable instructions for causing a programmable device to perform the method according to claim 1.